TINJAUAN *VIKTIMOLOGIS* TERHADAP KORBAN TINDAK PIDANA *CYBERCRIME ILLEGAL CONTENT* DI WILAYAH HUKUM POLRESTABES BANDUNG DIHUBUNGKAN DENGAN UNDANG-UNDANG NO 19 TAHUN 2016 TENTANG PERUBAHAN ATAS UNDANG-UNDANG NO 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

Nasrul Hamzah Jaelani, Utang Rosidin, M Irsan Nasution,
UIN Sunan Gunung Djati Bandung
Email: utangrosidin@uinsgd.ac.id, Nasutionm.irsan@uinsgd.ac.id

ABSTRAK

Illegal Contents Merupakan kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat diangap melanggar hukum atau mengganggu ketertiban umum. Bentuk tindak pidana *cybercrime* jenis ini tergolong pada situs bermuatan negatif, termasuk pula dalam kasus penghinaan dan pencemaran nama baik yang berisikan perkataan yang kasar dan tidak etis. Ketentuan mengenai penghinaan dan pencemaran nama baik diatur dalam Pasal 27 ayat (3) Undang-Undang No 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik, "Setiap orang dengan sengaja dan tanpa hak mendistribusikan atau mentransmisikan dan membuat dapat diaksesnya informasi elektronik dan dokumen elektronik yang memiliki muatan Penghinaan / Pencemaran Nama Baik". Tujuan penelitian ini adalah untuk mengetahui: (1). Kedudukan korban dalam tindak pidana cybercrime illegal content di wilayah hukum Polrestabes Bandung, (2). Perlindungan hukum terhadap korban tindak pidana *cybercrime illegal content* menurut Undang-Undang No 19 Tahun 2016 tentang Perubahan Atas Undang-Undang No 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik, (3). Upaya yang dilakukan oleh Polrestabes Bandung dalam menanggulangi adanya korban tindak pidana *cybercrime illegal content* di kota Bandung. Penelitian ini dilakukan dengan menggunakan metode *deskriptif analitis* dengan metode pendekatan *yuridis normative,* data diperoleh dari hasil penelitian studi pustaka dan penelitian lapangan, penelitian ini dilakukan di Wilayah Hukum Polrestabes Bandung. Hasil penelitian menunjukan bahwa; (1) Kedudukan korban dalam tindak pidana *cybercrime illegal content* adalah sebagai pelapor yang merasa telah dirugikan secara hukum dan kebanyakan korbannya adalah perempuan yang bekerja sebagai karyawan swasta, (2) Dalam perlindungannya, Undang-Undang No 11 Tahun 2008 tentang Informasi dan

Transaksi Elektronik tidak secara tegas dalam melindungi korban tindak pidana *cybercrime illegal content.* (3) Upaya yang dilakukan polrestabes bandung dalam menanggulangi adanya korban tindak pidana cybercrime illegal content dilakukan dengan dua cara, yaitu melalui upaya preventif (pencegahan) serta dengan upaya represif (penal), namun belum secara *efektive* dapat menanggulangi tindak pidana *cybercrime illegal content* dikarenakan berbagai hal diantaranya; alat yang dimiliki oleh aparat penegak hukum untuk mengungkap kasus *cybercrime* masih sangat terbatas jumlah dan penggunaannya, dan pelaku yang kerap menghilangkan barang bukti.

Kata Kunci : *Viktimologis,* Korban Tindak Pidana *Cybercrime Illegal Content*

A. PENDAHULUAN

Penggunaan sistem dan alat elektronik telah menciptakan suatu cara pandang baru dalam menyikapi perkembangan teknologi. Perubahan paradigma dari *paper based* menjadi *electronic based*. Dalam perkembangannya, *electronic based* semakin diakui keefisienannya, baik dalam hal pembuatan, pengolahan, maupun dalam bentuk penyimpanannya.[1] Perkembangan yang pesat dari teknologi telekomunikasi dan teknologi komputer menghasilkan internet yang multifungsi, perkembangan ini membawa kita keambang revolusi ke empat dalam sejarah pemikiran manusia bila di tinjau dari kontruksi pengetahuan umat manusia yang dicirikan dengan cara berfikir yang tanpa batas (*borderless way of thinking*). Internet merupakan simbol material Embrio masyarakat global. Internet membuat globe dunia, seolah-olah menjadi seperti hanya selebar daun kelor. Era reformasi ditandai dengan eksabilitas informasi yang amat tinggi. Dalam era ini, informasi merupakan komoditi utama yang diperjualbelikan sehingga akan muncul berbagai *network* dan *information company* yang akan memperjualbelikan fasilitas bermacam jaringan dan berbagai basis data informasi tentang berbagai hal yang dapat diakses oleh pengguna dan pelanggan. Internet menawarkan kepada manusia berbagai harapan dan kemudahan. Akan tetapi dibalik itu, timbul persoalan berupa kejahatan yang dinamakan *cybercrime*, baik sistem jaringan komputernya itu sendiri yang menjadi sasaran maupun komputer itu sendiri yang menjadi sarana untuk melakukan kejahatan. Tentunya jika kita melihat bahwa informasi itu sendiri telah menjadi komoditi maka upaya untuk

[1] Edmon Makarim, *Pengantar Hukum Telematika,* cet.I, PT. Raja Grafindo Persada: Jakarta, 2005, hlm. 447.

melindungi asset tersebut sangat diperlukan. Salah satunya dengan melalui hukum pidana, baik dengan bersarana penal maupun non penal.

Cybercrime merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian luas dari dunia internasional. Vollodymyr Golubev menyebutnya sebagai *the new form of anti-social behavior.* Kehawatiran terhadap ancaman (*threat*) *cybercrime* yang telah terungkap dalam makalah *Cybercrime* yang disampaikan dalam ITAC (*information Technology Association of Canada*) pada *International Information Industry Congress (IIC) 2000 Milenium Congres di* Quebec pada tanggal 19 September 2000, yang menyatakan bahwa *cybercrime is a real growing threat to economic and social development aspect of human life and so can electronically enabled crime*[2]. Kejahatan ini merupakan tindak kejahatan melalui jaringan sistem komputer dan sistem komunikasi baik lokal maupun global (internet) dengan memanfaatkan teknologi informasi berbasis sistem komputer yang merupakan sistem elektronik yang dapat dilihat secara virtual dengan melibatkan pengguna internet sebagai korbannya. Kejahatan tersebut seperti misalnya manipulasi data (*the trojan horse*), spionase, *hacking,* penipuan kartu keredit online (*carding)*, merusak sistem (*cracking*), dan berbagai macam lainnya. Pelaku *cybercrime* ini memiliki latar belakang kemampuan yang tinggi di bidangnya sehingga sulit untuk melacak dan memberantasnya secara tuntas.

Dewasa ini kita dapat melihat bahwa hampir seluruh kegiatan manusia mengandalkan teknologi yang menghadirkan kemudahan bagi penggunanya berupa akses bebas yang dapat dilakukan oleh siapapun, kapanpun dan dimanapun tanpa sensor serta ditunjang dengan berbagai penawaran internet murah dari penyedia jasa layanan internet. Kemudahan yang ditawarkan oleh aktivitas siber itu sendiri contohnya ketika melakukan jual-beli barang atau jasa tidak memerlukan lagi waktu yang lama untuk bertemu langsung dengan penjual atau pembelinya, sehingga waktu yang digunakan lebih cepat. Indonesia telah menggeser kedudukan Ukraina sebagai pemegang presentasi tertinggi terhadap *cybercrime.* Data tersebut berasal dari penelitian Verisgin, perusahaan yang memberikan pelayanan intelejen di dunia maya yang berpusat di California, Amerika Serikat. Hal ini juga ditegaskan oleh Staf Ahli Kapolri Brigjen Anton Tabah bahwa jumlah *cybercrime* di Indonesia adalah yang tertinggi di dunia. Indikasinya dapat dilihat dari banyaknya kasus

[2] Barda Nawawi Arief, *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime Di Indonesia*, PT Raja Grafindo Persada: Jakarta, 2006, hlm. 2.

pemalsuan kartu kredit, penipuan perbankan, judi *online*, terorisme, dan lain-lainnya.[3]

Memanfaatkan teknologi dalam kehidupan sehari-hari telah menjadi gaya hidup masyarakat kita, akan tetapi penggunaan teknoligi tersebut tidak didukung dengan pengetahuan untuk menggunakannya dengan baik. Hasil Lembaga Riset Telematika Sharing Vision menempatkan Tahun 2013 Indonesia menjadi negara urutan pertama target kejahatan dunia maya. Hasil riset itu menyebutkan selama Tahun 2013 ada 42 ribu serangan *cyber* saban harinya. Dimitri Mahayana dalam seminar '*Indonesia Cyber Crime Summit* 2014' di ITB menyebutkan bahwa saat ini masyarakat Indonesia menduduki peringkat pertama dunia dengan persentase sebesar 23,54 persen sebagai pengguna internet terbesar.[4] Setiap terjadi kejahatan maka dapat dipastikan akan menimbulkan kerugian pada korbannya. Korban kejahatan menanggung kerugian karena kejahatan, baik materiil maupun immateriil. Korban kejahatan yang pada dasarnya merupakan pihak yang paling menderita dalam suatu tindak pidana, tidak memperoleh perlindungan sebanyak yang diberikan oleh undang-undang kepada pelaku kejahatan. Akibatnya, pada saat pelaku kejahatan telah dijatuhi sanksi pidana oleh pengadilan, kondisi korban kejahatan tidak dipedulikan.[5] Kerugian baik materiil maupun immateriil yang ditimbulkan bernilai sangat besar dan dalam waktu yang relatif singkat bila dibandingkan dengan kejahatan konvensional yang lebih mudah dilokalisir. Sehingga diperlukan upaya penanggulangan bagi kejahatan teknologi informasi ini baik upaya pencegahan kejahatan secara preventif maupun penanggulangan kejahatan secara represif. Kehadiran hukum pidana sangat diperlukan agar dapat mengatasi *cybercrime* yang semakin berkembang. Upaya penanggulangan tersebut sewajarnya menjadi jaminan bagi pengguna internet agar dapat melakukan aktivitas *cyber* dengan nyaman dan aman serta diharapkan kepada seluruh masyarakat dapat turut aktif. Menurut Mochtar Kusumaatmadja[6], hukum mempunyai kekuasaan untuk melindungi dan mengayomi seluruh lapisan masyarakat sehingga tujuan hukum dapat tercapai dalam mewujudkan keadilan sosial bagi seluruh rakyat Indonesia dan

[3] Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya,* Rajawali Pers: Jakarta, 2013, hlm. 17.

[4] http://www.merdeka.com/peristiwa/hasil-riset-hukum-tahun-2013-Indonesia-target-utama-kejahatan-cyber.httml, diakses pada 15 Maret 2017.

[5] Dikdik M. Arief Mansur & Eliksatris Gultom, *Urgensi Perlindungan Korban Kejahatan,* PT. Raja Grafindo Persada: Jakarta, 2007, hlm. 24

[6] Budi Suhariyanto, *Op.Cit,* hlm. 99

sekaligus berfungsi sebagai sarana penunjang perkembangan pembangunan secara menyeluruh. Teknologi informasi seharusnya memberikan manfaat dan kesejahteraan untuk menunjang aktivitas sehari-hari, maka dengan konsepsi tersebut pemanfaatan teknologi informasi harus berdasarkan pada asas-asas yang dimuat dalam Pasal 3 Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang selanjutnya disingkat dengan (UU ITE) yaitu: Pemanfaatan Teknologi Informasi dan Transaksi Elektronik dilaksanakan berdasarkan asas kepastian hukum, manfaat, kehati-hatian, itikad baik, dan kebebasan memilih teknologi atau netral teknologi. Selanjutnya pada Pasal 15 menyatakan : 1) Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya. 2) Penyelenggara Sistem Elektronik bertanggung jawab terhadap Penyelenggaraan Sistem Elektroniknya. 3) Ketentuan sebagaimana dimaksud pada ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik.

Illegal Content merupakan salah satu bentuk pengelompokan kejahatan yang berhubungan dengan teknologi informasi (TI). *Illegal Content* dapat di definisikan sebagai kejahatan dengan memasukan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Dalam artian sederhana, adalah merupakan kegiatan menyebarkan seperti mengunggah dan menulis hal yang salah atau dilarang yang dapat merugikan orang lain.[7] Pentingnya pengaturan *illegal content* dalam UU ITE didasarkan setidaknya pada dua hal. Pertama, perlunya perlindungan hukum seperti perlindungan yang diberikan dalam dunia nyata atau fisik (*real space*). Dunia siber merupakan dunia virtual yang diciptakan melalui pengembangan teknologi informasi dan komunikasi. Pada dasarnya konten merupakan informasi yang dapat mempengaruhi perilaku seseorang. Pornografi dan judi dapat menimbulkan kecanduan, pembuatan informasi elektronik khususnya pornografi dapat atau bahkan sering melanggar hak asasi manusia. Selain itu penyebaran konten dapat membentuk opini publik. Rusaknya kehormatan atau nama baik seseorang akibat opini publik yang terbentuk melalui penyerangan terhadap kehormatan atau nama baik orang tersebut merupakan

[7] Barda Nawawi Arief, *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime Di Indonesia*, PT Raja Grafindo Persada: Jakarta, 2006, hlm. 42.

alasan diaturnya ketentuan penghinaan dalam *cyberspace*. Kerusuhan antar suku, agama, ras, dan golongan (SARA) juga dapat terjadi akibat penyebarluasan informasi sensitive tentang SARA. Kedua, dengan adanya internet, informasi dapat disebar dan diteruskan ke berbagai penjuru dunia dengan seketika serta dapat diakses dari berbagai Negara. Terlebih lagi setiap orang dapat menggunakan nama lain selain nama diri yang sebenarnya di *cyberspace* baik secara anonym atau dengan nama samaran. Yang dimaksud dalam *illegal content* menurut undang-undang ini adalah informasi atau dokumen elektronik yang memiliki muatan yang melanggar kesusilaan, perjudian, penghinaan, atau pencemaran nama baik, dan pemerasan atau pengancaman sebagai mana termuat dalam pasal 27 UU ITE. Dalam Pasal 27 Undang-Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, menyatakan: 1) Setiap orang "dengan sengaja dan tanpa hak mendistribusikan atau mentransmisikan atau membuat dapat diaksesnya informasi elektronik atau dokumen elektronik yang memiliki muatan yang melanggar kesusilaan". 2) Setiap orang dengan sengaja dan tanpa hak mendistribusikan atau mentransmisikan dan membuat dapat diaksesnya informasi elektronik dan dokumen elektronik yang memiliki muatan perjudian. 3) Setiap orang dengan sengaja dan tanpa hak mendistribusikan atau mentransmisikan dan membuat dapat diaksesnya informasi elektronik dan dokumen elektronik yang memiliki muatan Penghinaan / Pencemaran Nama Baik. 4) Setiap orang dengan sengaja dan tanpa hak mendistribusikan atau mentransmisikan dan membuat dapat diaksesnya informasi elektronik dan dokumen elektronik yang memiliki muatan pemerasan atau pengancaman.[8]

Akhir-akhir ini sering terjadi penyebaran hal-hal yang tidak teruji kebenaran akan faktanya yang tersebar bebas di internet, baik itu dalam bentuk foto, video maupun berita-berita. Dalam hal ini tentu saja mendatangkan kerugian bagi pihak yang menjadi korban dalam pemberitaan yang tidak benar tersebut, seperti kita ketahui pasti pemberitaan yang beredar merupakan berita yang sifatnya negatif. Dalam beberapa tahun terakhir ini marak terjadi pemberitaan yang tidak benar *(Hoax)* diantaranya yang menimpa walikota Bandung Ridwan Kamil. Sang walikota Bandung pun segera merespon tindakan tersebut melalui akun media sosial. Dan segera melaporkan kepada pihak yang berwajib. Sebelumnya Wali Kota Bandung Ridwan Kamil mengakui kesal mendapat serangan secara terbuka dan kasar

[8] Undang-Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

di media sosial. Tulisan akun itu dinilainya sudah menyerang pribadinya. Ridwan membantah sedang mencari sensasi atau terlalu reaktif. Pria yang akrab disapa kang Emil ini mengaku sudah biasa dicaci maki. Selain berisi nada hinaan, akun tersebut juga mengundang ancaman.[9]

Dari kasus tersebut dapat disimpulkan jika kasus penghinaan terhadap orang lain merupakan salah satu jenis *cybercrime* yang dapat dikategorikan kedalam *illegal content*. Perbuatan dalam kasus ini terdapat dalam Undang-Undang No 19 Tahun 2016 tentang Perubahan Atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; Pasal 27 ayat (3) yang berbunyi "Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Eletronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik." Ketentuan pidana dalam kasus ini terdapat dalam Pasal 45 ayat (3) yang berbunyi "Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Eletronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik sebagaimana dimaksud dalam Pasal 27 ayat (3), dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp 750.000.000,00 (tujuh ratus lima puluh juta rupiah)." Yang menarik dari proses hukum dalam tindak pidana "*Illegal Content*" ini ialah hanya pelaku penyebaran, pengunggahan, atau penghinaan di media sosial saja yang mendapat sanksi pidana kemudian dianggap selesai. sedangkan tidak ada perhatian khusus terhadap korban, sehingga korban muncul sebagai orang yang dilupakan serta sebagai individu yang dirugikan.

B. TINJAUAN TEORITIS

1. Pengertian Viktimologi

Menurut Kamus Hukum *Law Dictionary* Victim adalah "orang yang telah medapat penderitaan fisik atau penderitaan mental, kerugian harta benda atau mengakibatkan mati atas perbuatan atau usaha pelanggaran ringan dilakukan oleh pelaku tindak pidana dan lainya.[10] Korban dalam pengertian yurdis yang termaktub dalam perundang-undangan No.13 Tahun 2006 tentang perlindungan saksi dan korban adalah seseorang yang mengalami penderitaan

[9]https://news.detik.com/berita-jawa-barat/d-3452789/dituduh-syiah-di-medsos-ridwan-kamil-laporkan-pemilik-akun

[10] Bambang Waluyo, *Viktimologi Perlindungan Korban dan Saksi,* Jakarta, 2011, hlm. 9

fisik, mental, dan/atau kerugian ekonomi yang diakibatkan oleh suatu tindak pidana". [11] Menurut Ahli hukum yang mengutip pendapat Schafer menyatakan bahwa perkembangan perhatian terhadap korban atau *victim* telah dimulai sejak abad pertengahan. Perhatian terhadap korban kejahatan ini kemudian merupakan embrio kelahiran dari suatu cabang ilmu baru yang dikenal dengan *victimology*.[12] Viktimologi berasal dari bahasa Latin *victima* yang artinya korban dan *logos* yang artinya ilmu. Secara terminologis, viktimologi berarti suatu studi yang mempelajari tentang korban, penyebab timbulnya korban dan akibat-akibat penimbulan korban yang merupakan masalah manusia sebagai suatu kenyataan sosial.[13] Menurut Arief Gosita, pengertian Viktimologi adalah suatu pengetahuan ilmiah/studi yang mempelajari suatu viktimisasi (kriminal) sebagai suatu permasalahan manusia yang merupakan suatu kenyataan sosial[14].

2. Pengertian Korban Kejahatan

Menurut Kamus Besar Bahasa Indonesia (KBBI) yang dimaksud korban kejahatan adalah: a) Korban; Orang, binatang, dan sebagainya yang menjadi menderita (mati dan sebagainya) akibat suatu kejadian, perbuatan jahat, dan sebagainya. b) Kejahatan; *Istilah hukum* perbuatan yang jahat: korupsi, merampok, dan mencuri merupakan kejahatan yang melanggar hukum; sifat yang jahat; perilaku yang bertentangan dengan nilai dan norma yang berlaku yang telah disahkan oleh hukum tertulis. Dalam Kamus Hukum (*Law Dictiory)* yang dimaksud dengan kejahatan adalah tindak pidana yang tergolong berat lebih berat dari sekedar pelanggaran, perbuatan yang sangat anti sosial yang oleh negara dengan sadar menjatuhkan hukuman kepada pelakunya; perbuatan jahat; sifat yang jahat.[15] Menurut Arif Gosita[16], yang dimaksud dengan korban adalah mereka yang menderita jasmaniah dan rohaniah sebagai akibat tindakan orang lain yang mencari pemenuhan kepentingan diri sendiri atau orang lain yang bertentangan dengan kepentingan dan hak asasi yang mederita.

---

[11] *Op.Cit.* hlm. 9.

[12] Romli Atmasasmita, *Teori dan Kapita Selekta Kriminologi* , PT Eresco: Bandung, 1992, hlm 7.

[13] Dikdik M. Arief Mansur dan Elisatris Gultom, *Op.Cit.*, hlm. 34.

[14] Arif Gosita, *Masalah Korban Kejahatan (Kumpulan Karangan)*, Akademika Pressindo: Jakarta,1993, hlm. 40

[15] Media Internet, (*https://kamushukum.web.id/search/kejahatan),* diakses pada tanggal 20 Oktober 2017

[16] Arif Gosita, *Op. Cit.*, hlm. 63

3. Tindak Pidana *Cybercrime Illegal Content*

Sistem teknologi informasi berupa internet telah dapat menggeser paradigma para penegak hukum terhadap definisi kejahatan komputer sebagaimana ditegaskan sebelumnya, bahwa pada awalnya para ahli hukum terfokus pada alat/ perangkat keras yaitu komputer. Namun dengan adanya perkembangan teknologi informasi berupa jaringan internet, maka fokus dari indentifikasi terhadap definisi *cybercrime* lebih diperluas lagi yaitu seluas aktivitas yang dapat dilakukan di dunia *cyber*/maya melalui sistem informasi yang digunakan. Jadi tidak sekedar komponen *hardware*nya saja kejahatan tersebut dimaknai sebagai *cybercrime*, tetapi sudah dapat diperluas dalam lingkup dunia yang dijelajah oleh suatu sistem teknologi informasi yang bersangkutan Sehingga akan lebih tepat jika pemaknaan dari *cybercrime* adalah kejahatan teknologi informasi.[17] Secara umum, yang dimaksud kejahatan di dunia *cybercrime* (*cybercrime*) adalah upaya memasuki dan atau menggunakan fasilitas komputer atau jaringan komputer tanpa ijin dan dengan melawan hukum dengan atau tanpa menyebabkan perubahan dan atau kerusakan pada fasilitas komputer yang dimasuki atau digunakan tersebut.[18]

4. Ketentuan Hukum Dalam *Cybercrime Illegal Content*

Sebagai langkah preventif terhadap segala hal yang berkaitan dengan tindak pidana di bidang komputer khususnya *cybercrime illegal content*, sedapat mungkin dikembalikan pada peraturan perundang-undangan yang ada, yaitu KUHP (Kitab Undang-undang Hukum Pidana) dan peraturan di luar KUHP. Pengintegrasian dalam peraturan yang sudah ada berarti melakukan suatu penghematan dan mencegah timbulnya *over criminalization*[19], tanpa mengubah asas-asas yang berlaku dan tidak menimbulkan akibat-akibat sampingan yang dapat mengganggu perkembangan teknologi informasi.

C. METODE PENELITIAN

Dalam penelitian ini penulis akan menggunaka Metode Penelitian menggunakan metode deskriptif analitis, menggunakan metode pendekatan *yuridis normatif*, penelitian hukum yang menggunakan teori/konsep dan asas-

[17] Budi Suhariyanto,*Op. Cit*., hlm. 10-11

[18] Dikdik M. Arief Mansur dan Elisatris Gultom, *Op. Cit*., hlm. 8

[19] Marjono Reksodiputro, *Kemajuan Pembangunan Ekonomi dan Kejahatan*, Pusat Pelayanan Keadilan dan Pengabdian Hukum: Jakarta, 1994, hlm. 13

asas hukum. Tahap Penelitian dilakukan dalam 2 (dua) tahapan, yaitu: 1) Penelitian Kepustakaan (*Library Research)* dan 2) Penelitian Lapangan (*Field Research). Pengumpulan data* yang dilakukan dengan cara mencari dan menyimpulkan data baik literatur, wawancara, maupun perundang-undangan yang berkaitan dengan permasalahan yang diteliti. Analisis data menggunakan analisis *yuridis kualitatif*.

D. HASIL DAN PEMBAHASAN

1. Kedudukan Korban Dalam Tindak Pidana *Cybercrime Illegal Content* di Wilayah Hukum Polrestabes Bandung

a. Perkembangan Tindak Pidana *Cybercrime Illegal Content* di Kota Bandung

Illegal Contents Merupakan kejahatan dengan memasukan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat diangap melangar hukum atau mengganggu ketertiban umum. Bentuk tindak pidana *cybercrime* jenis ini tergolong pada situs bermuatan negatif, termasuk pula dalam kasus penipuan yang memuat hal tidak benar serta penghinaan dan pencemaran nama baik yang berisikan perkataan yang kasar dan tidak etis. Ketentuan mengenai penghinaan dan pencemaran nama baik diatur dalam Pasal 27 ayat (3) Undang-Undang No 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik. Tindak pidana *Cybercrime Illegal Content* merupakan permasalahan yang berkembang di dunia modern. Semakin modern kehidupan masyarakatnya maka semakin beragam dan modern juga modus kejahatannya. Masyarakat modern umumnya merupakan masyarakat perkotaan yang berorientasi dengan perkembangan zaman masa kini terutama dalam hal pengetahuan dan teknologi, tidak terkecuali kota besar seperti Kota Bandung. Salah satu faktor pendorong terjadinya tindak pidana *Cybercrime Illegal Content* adalah kemajuan teknologi itu sendiri yang penggunanya semakin hari semakin bertambah namun tidak diiringi dengan pengetahuan penggunaannya. *Cybercrime Illegal Content* adalah kejahatan konvensional teknologi informasi yang terjadi di ruang virtual atau maya yang dapat meresahkan penggunanya, kerugian yang diakibatkan tindak pidana ini dapat berupa materiil yang tidak sedikit dan imateriil yang kemudian berdampak secara psikologi terhadap korban.

Secara umum dapat dijelaskan bahwa jumlah perkara tindak pidana *cybercrime illegal content* yang dilaporkan di kota Bandung mengalami peningkatan. Peningkatan terjadi pada awal tahun 2017 pada bulan Januari sebanyak 4 kasus kemudian menurun pada bulan-bulan berikutnya sampai

meningkat kembali pada bulan Mei sebanyak 4 kasus. Menurut BA Urbin Ops Satreskrim Aipda Teddy Yuliadi, peningkatan tersebut disebabkan karena sudah banyak masyarakat yang telah menggunakan media elektronik dan juga didukung dengan harga yang relatif tejangkau, akan tetapi hal tersebut disalahgunakan. Dalam 1 tahun terakhir tercatat telah terjadi 16 kasus *cybercrime illegal content* yang dilaporkan, jumlah tersebut masih relatif rendah peningkatan pertahunnya. namun, jika dibiarkan tidak menutup kemungkinan bahwa akan terjadi peningkatan yang cukup tinggi pada tahun-tahun selanjutnya seiring semakin majunya teknologi, seperti pada akhir tahun 2016 sampai awal tahun 2017. Oleh karena itu, diperlukan kerjasama antara korban dan pihak-pihak terkait sehingga kejahatan ini terus berkurang dan menciptkan rasa aman dan nyaman saat menggunakan media informasi elektronik. Sementara itu, Penulis juga mendapatkan data laporan masyarakat khusus wilayah kota Bandung kepada Polda Jabar yang memiliki unit khusus menangani kasus Ditreskrimsus *Cybercrime* dimana penulis melakukan penelitian bahwa pada tahun 2015/2016 terjadi peningkatan kasus *cybercrime* khususnya *illegal content* sebanyak 124 kasus dan merupakan yang tertinggi dalam 2 tahun terakhir. 77 kasus diantaranya telah diselesaikan dengan penetapan 77 tersangka dan telah dilimpahkan ke Pengadilan.

Modus dari tindak pidana *cybercrime* semakin hari semakin beragam dan canggih sehingga kejahatan ini juga ikut berkembang. Menurut hasil wawancara dengan Iptu Ali Jupri, SH, MH selaku Kanit Idik 1 Satreskrim Polrestabes Bandung (07 Juni 2017), tindak pidana terbanyak yang dilaporkan oleh korban adalah mengenai penghinaan dan pencemaran nama baik. Hal senada juga disampaikan oleh Teddy Yuliadi yang menyebutkan bahwa 1 tahun terakhir dari laporan masyarakat yang diterima terkait *cybercrime*, penghinaan dan pencemaran nama baik menempati posisi pertama dengan persentase 60%, lalu diikuti dengan penipuan sebesar 35% dan sisanya terdapat kasus lain seperti perjudian melalui internet, pemerasan, penyebaran gambar porno, peretasan atau *hacking* sebesar 5%. Penghinaan dan pencemaran nama baik menempati posisi teratas dalam bentuk kejahatan *cybercrime illegal content.* Kebebasan berpendapat atau mengkritisi suatu permasalahan jika tidak diutarakan dengan baik dapat menjadi pemicu pelanggaran pidana jenis ini. Batasan antara berpendapat atau mengkritisi suatu masalah dengan melakukan penghinaan dewasa ini sangat tipis perbedaan diantara keduanya. Penghinaan dan pencemaran nama baik merupakan delik aduan mutlak, karena ketika kritik atau pendapat tersebut menyinggung pihak yang merasa dirugikan dan dilaporkan barulah

perbuatan tersebut termasuk tindak pidana dan menjadi mutlak karena yang dilaporkan dan dituntut adalah perbuatannya. Dengan demikian, dapat disimpulkan bahwa perkembangan tindak pidana *cybercrime illegal content* di kota Bandung mengalami peningkatan di setiap tahunnya. Paling banyak laporan tentang pencemaran nama baik yang diatur dalam Pasal 27 ayat (3) Undang-Undang ITE. Berbagai hal yang menjadi penyebab meningkatnya kasus ini, akan tetapi faktor yang paling besar yakni meningkatnya pengguna media social/elektronik yang tidak sesuai dengan fungsi penggunaannya.

b. Kedudukan Korban Dalam Tindak Pidana *Cybercrime illegal content* di Wilayah Hukum Polrestabes Bandung

Sistem peradilan pidana di Indonesia cenderung kepada pendekatan kontrol sosial, di mana monopoli penuntutan terhadap pelaku perbuatan pidana dipegang oleh negara. Kedudukan korban dalam sistem peradilan pidana maupun dalam praktik peradilan relatif kurang diperhatikan karena ketentuan hukum Indonesia masih bertumpu pada perlindungan bagi pelaku (*offender orientied*). Sebagaimana diketahui bahwa Undang undang Nomor : 8 tahun 1981, tentang Hukum Acara Pidana manganut sistem peradilan pidana yang mengutamakan Perlindungan hak hak azasi manusia, namun apabila ketentuan ketentuan mengenai hal itu diperhatikan secara lebih mendalam, ternyata hanya hak hak tersangka/terdakwa yang banyak ditonjolkan sedangkan hak hak dari korban kejahatan sangat sedikit diatur. Sejalan dengan azas tersebut masyarakat khususnya media massa lebih banyak menyoroti mengenai hak hak tersangka/terdakwa dari pada mempermasalahkan mengenai Perlindungan terhadap korban kejahatan. Padahal, dari pandangan kriminologis dan hukum pidana kejahatan adalah konflik antar individu yang menimbulkan kerugian kepada korban, masyarakat dan pelanggar sendiri dimana dari ketiga kelompok itu kepentingan korban kejahatan adalah bagian utama kejahatan dimana menurut Andrew Ashworth, "*primary an offence against the victim and only secondarily an offence against the wider comunity or state*".

Bahkan secara umum publik memiliki pandangan yang menyebutkan pada saat pelaku kejahatan telah diperiksa, diadili dan dijatuhi hukuman pidana, maka pada saat itulah perlindungan terhadap korban telah diberikan, padahal pendapat demikian tidak sepenuhnya benar. Hal ini secara umum tercermin dalam setiap penanganan perkara pidana oleh aparat penegak hukum (polisi, jaksa) seringkali dihadapkan pada kewajiban untuk melindungi dua kepentingan yang terkesan saling berlawanan, yaitu kepentingan korban yang harus dilindungi untuk memulihkan

penderitaannya karena telah menjadi korban kejahatan (secara mental, fisik, maupun material), dan kepentingan tertuduh/tersangka sekalipun dia bersalah tetapi dia tetap sebagai manusia yang memiliki hak asasi yang tidak boleh dilanggar. Apalagi dalam hal perbuatannya itu belum memperoleh putusan hakim yang menyatakan bahwa pelaku bersalah, pelaku harus dianggap sebagai orang yang tidak bersalah (azas praduga tidak bersalah). Korban kejahatan yang pada dasarnya merupakan pihak yang paling menderita dalam suatu tindak pidana, karena tidak memperoleh perlindungan sebanyak yang diberikan oleh undang-undang kepada pelaku kejahatan. Singkatnya, dalam membahas hukum acara pidana khususnya yang berkaitan dengan hak-hak asasi manusia, ada kecenderungan untuk mengupas hal-hal yang berkaitan dengan hak-hak tersangka tanpa memperhatikan pula hak-hak para korban. Oleh karena itu pemikiran viktimologi memberikan dasar mengenai perlunya korban diberi pelayanan yang memungkinkan untuk mendapatkan pelayanan kepentingan yang diperlukan korban.

Viktimologi menganalisis mengenai berbagai aspek yang berkaitan dengan korban kejahatan, bagaimana seseorang tersebut dapat menjadi korban dari suatu kejahatan dengan kata lain merujuk kepada kedudukan korban dalam terjadinya kejahatan, salah satunya adalah *cybercrime illegal content*. Korban tindak pidana *cybercrime* ini tidak hanya menyerang individu ataupun kelompok masyarakat tetapi juga dapat menyerang badan usaha. Kedudukan korban dalam kejahatan *cybercrime illegal content* juga beragam mengikut jenis tindak pidana *cybercrime illegal content* yang dilakukan oleh pelaku. Menurut klasifikasi atau tipologi korban, korban tindak pidana *cybercrime* termasuk dalam tipe *participacing victim*. *Participating victims* adalah mereka yang tidak menyadari atau memiliki perilaku lain sehingga memudahkan dirinya menjadi korban. Menurut hasil wawancara dengan Teddy Yuliadi menjelaskan mengenai kedudukan korban dalam terjadinya *cybercrime illegal content*.

Berdasarkan hal ini maka kedudukan korban terbagi dalam beberapa faktor yang pertama dari umur, rata-rata korban berusia dewasa menurut undang-undang atau telah cakap hukum, dalam dua tahun terakhir ini belum ada laporan mengenai tindak pidana *cybercrime illegal content* yang menimpa anak-anak dibawah umur. Kemudian dari jenis kelamin korban kebanyakan adalah perempuan dibandingkan dengan laki-laki dengan pekerjaan rata-rata sebagai karyawan swasta. Dalam kedudukan hukumnya korban ditempatkan sebagai alat bukti yang memberi keterangan yaitu hanya sebagai saksi, sehingga kemungkinan bagi korban untuk memperoleh keleluasaan dalam

memperjuangkan haknya adalah kecil. Korban tidak diberikan kewenangan dan tidak terlibat secara aktif dalam proses penyidikan dan persidangan, sehingga ia kehilangan kesempatan untuk memperjuangkan hak-haknya dan memulihkan keadaanya. Akibatnya, pada saat pelaku telah dijatuhi sanksi pidana oleh pengadilan, kondisi korban seperti tidak dipedulikan sama sekali. Adapun faktor-faktor yang menyebabkan terjadinya korban tindak pidana *cybercrime illegal content*. Teddy Yuliadi menjelaskan lebih rinci mengenai faktor pertama, yaitu hubungan antara keluarga, teman ataupun relasi. Hal ini menjadi penyebab utama dikarenakan korban memliki masalah sebelumnya dengan lingkungan sosialnya, sehingga dapat memicu amarah ataupun kata-kata yang tidak pantas diucapkan. Tidak hanya itu saja, lebih lanjut menurut Iptu Ali Jupri, SH, hubungan dengan relasi yang tidak harmonis atau melakukan hal yang tidak disukai oleh pelaku serta adanya persaingan baik di bidang politik ataupun sosial diantara kedua belah yang berujung dengan saling menjatuhkan pihak lawan. Di antara korban yang menjadi korban penghinaan akibat hubungan yang tidak harmonis paling banyak dialami oleh masyarakat biasa dan pelakunya masih memiliki hubungan keluarga dengan korban. Seorang korban bernama Reni (mahasiswi, 1 tahun) berdasarkan wawancara (25 Mei 2017) menerangkan bahwa dirinya pernah menjadi korban pencemaran nama baik di media sosial. Pelaku memasukan foto korban ke salah satu media sosial dan meminta pendapat dari pengguna lainnya mengenai diri korban di media sosial tersebut. Diantara komentar yang masuk, hanya pelaku lah yang menuliskan kata-kata tidak pantas dan melecehkan korban. Tidak hanya sampai disitu saja korban juga terkadang menerima pesan yang sama dan terkesan mengancam. Korban mengetahui bahwa fotonya menjadi bulan-bulanan pelaku dari temannya yang mengenal foto dirinya. Korban tidak mengetahui siapa yang mengunggah foto tesebut, ia merasa dirinya tidakpernah bermasalah dengan siapapun.

Faktor yang kedua yaitu mengenai pengetahuan akan teknologi informasi yang digunakan oleh penggunanya. Menurut Iptu Ali Jupri, teknologi yang semakin berkembang tidak diimbangi dengan pengetahuan penggunanya, faktor ini biasanya terkait dengan penipuan. Korban yang tujuan awalnya mencari kebutuhannya kemudian tertarik terhadap barang atau jasa yang ditawarkan tetapi tidak mengetahui apakah barang ditawarkan itu ada atau tidak, legal atau ilegal atau situs yang digunakan bersifat asli atau palsu. Pelaku melihat kesempatan yang diberikan korban yang mulai tertarik dengan barang yang ditawarkan, mengingat bahwa kegiatan jual beli barang atau jasa di internet antara penjual dan pembeli tidak pernah bertemu secara langsung.

Aipda Teddy Yuliadi memberikan penjelasan yang senada, bahwa ketika melakukan pembelanjaan secara *online* kebanyakan pembeli tidak mengetahui bagaimana cara aman untuk melakukan transaksi secara aman dan rahasia, seperti memasukkan nomor kartu kredit pada situs yang belum diketahui keasliannya sehingga nomor kartu kredit bisa tersalin ke suatu sistem yang disiapkan oleh pelaku kejahatan. Faktor ketiga yaitu kelalaian, menurut Iptu Ali Jupri hal ini juga berkaitan dengan faktor sebelumnya. Korban terkadang lalai karna tidak mengetahui perbuatannya, seperti meninggalkan akun pribadinya dan tidak menutupnya sesuai dengan prosedur yang ditetapkan sehingga sewaktu-waktu orang lain bisa menggunakan akun tersebut untuk melakukan kejahatan. Teddy Yuliadi kemudian mengatakan bahwa kelalaian dapat membuka kesempatan yang besar kepada pelaku untuk melakukan kejahatan dan merugikan korban. Jika korban lalai pada kasus-kasus seperti *hacking*, membiarkan sistem terbuka dan tidak dengan segera mengamankan data pelaku dapat dengan cepat mengambil ataupun merubah sistem, karna pelaku dapat melihat kelemahan dari sistem keamanan yang dibangun atau dibuat oleh korban. Setelah penulis melakukan wawancara dengan korban tindak pidana *cybercrime illegal content*, banyak dari mereka mengatakan kalau kasusnya tidak dapat dilanjutkan hal ini dikarenakan kekurangan alat bukti dan pelakunya pun tidak dapat diserahkan kepada pihak yang berwajib. Berkaitan dengan hal tersebut, Iptu Ali Jupri membenarkan bahwa terdapat beberapa kendala dalam pengungkapan kasus tersebut. Seperti misalnya, pelaku menghilangkan alat bukti berupa *simcard* yang digunakan untuk melakukan kejahatan. Hal ini memberatkan penyidikan untuk mengunkpa keberadaan dari pelaku, bisa jadi pelaku berada hari ini di kota A dan berikutnya terlacak di kota B dan juga pihak dari kejaksaan tidak menerima jika alat bukti belum lengkap. Tempat kejahatan atau *locus delicti* untuk kejahatan ini bersifat maya, berada di sebuah ruang virtual yang sangat sulit untuk menemukan barang bukti jika dihilangkan oleh pelaku. Alat yang digunakan pun masih sangat terbatas penggunannya dan jumlahnya sangat sedikit serta mengingat kasus seperti ini bisa terjadi dimana saja (transnasional) jadi butuh koordinasi terlebih dahulu dengan daerah dimana pelaku terakhir berada. Fakta lain yang ditemukan setelah penulis melakukan wawancara adalah banyak dari korban tindak pidana *cybercrime illegal content* tidak melaporkan kasusnya kepada pihak yang berwajib dan merelakan kejadiannya berlalu begitu saja dengan lebih berhati-hati untuk selanjutnya atau menyelesaikan masalahnya sendiri, seperti menemui langsung pelaku dan meminta pertanggungjawabannya. Para korban beranggapan bahwa

polisi tidak akan bisa menangkap pelakunya, dikarenakan korban mengetahui teknologi yang dimiliki oleh kepolisian belum memadai dan membuang waktu. Dengan demikian, berdasarkan analisis penulis, kedudukan korban dalam tindak pidana *cybercrime illegal content* di wilayah hukum Polrestabes Bandung adalah sebagai pihak yang secara hukum telah dilanggar hak-haknya menyangkut data pribadi/ kehormatan dirinya (*privacy)* karena suatu penghinaan, pencemaran nama baik, ataupun penyebaran konten asusila melalui media sosial/elektronik yang kebanyakan korbannya menimpa perempuan dan kedudukan hukumnya dalam proses persidangan, korban dijadikan sebagai alat bukti yang memberikan keterangan sebagai saksi.

2. Perlindungan Hukum Terhadap Korban Tindak Pidana *Cybercrime Illegal Content* Menurut Undang-Undang No 19 Tahun 2016 tentang Perubahan Atas Undang-Undang No 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik

Berdasarkan Undang-Undang No. 13 Tahun 2006 tentang Perlindungan Saksi dan Korban yang dimaksud dengan Perlindungan dijelaskan dalam Bab 1 Ketentuan Umum Pasal 1 ayat (6) bahwa; Perlindungan adalah segala upaya pemenuhan hak dan pemberian bantuan untuk memberikan rasa aman kepada Saksi dan/atau Korban yang wajib dilaksanakan oleh LPSK atau lembaga lainnya sesuai dengan ketentuan Undang-Undang ini. Perlindungan terhadap korban haruslah menjadi perhatian khusus baik dari pemerintah, pelaku pembuat Undang-Undang, aparat penegak hokum (kepolisian), badan hokum (peradilan), maupun masyarakat, sehingga korban tidak muncul sebagai orang yang dilupakan serta sebagai individu yang dirugikan. Terciptanya keseimbangan antara perlindungan korban kejahatan dengan pelaku kejahatan merupakan salah satu tujuan dari hokum itu sendiri, karena pada dasarnya ketidak-seimbangan merupakan salah satu pengingkaran dari asas setiap warga negara yang bersamaan kedudukannya dalam hukum dan pemerintahan, sebagaimana diamanatkan oleh Undang-undang Dasar 1945, sebagai landasan konstitusional. Memulihkan kepercayaan Warga Negara Indonesia terhadap pelaksanaan hukum yang diselenggarakan oleh Negara demi terciptanya rasa keadilan yang hakiki, serta menciptakan efek jera kepada pelaku tindak pidana. Delik kejahatan internet (*cybercrime)* yang diatur dalam Undang-Undang No 19 Tahun 2016 tentang Perubahan Atas Undang-Undang No 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik yang selanjutnya disingkat dengan (UU ITE), antara lain:

a. Tindak pidana yang berhubungan dengan aktivitas ilegal, yaitu:
1) Distribusi atau penyebaran, transmisi, dapat diaksesnya konten ilegal, yang terdiri dari: a) Kesusilaan (Pasal 27 ayat [1] UU ITE); b) Perjudian (Pasal 27 ayat [2] UU ITE); c) Penghinaan atau pencemaran nama baik (Pasal 27 ayat [3] UU ITE); d) Pemerasan atau pengancaman (Pasal 27 ayat [4] UU ITE); e) Berita bohong yang menyesatkan dan merugikan konsumen (Pasal 28 ayat [1] UU ITE); f) Menimbulkan rasa kebencian berdasarkan SARA (Pasal 28 ayat [2] UU ITE); g) Mengirimkan informasi yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi (Pasal 29 UU ITE);
   a) Dengan cara apapun melakukan akses ilegal (Pasal 30 UU ITE);
   b) Intersepsi ilegal terhadap informasi atau dokumen elektronik dan Sistem Elektronik (Pasal 31 UU ITE);
b. Tindak pidana yang berhubungan dengan gangguan (interferensi), yaitu:
   1) Gangguan terhadap Informasi atau Dokumen Elektronik (*data interference* – Pasal 32 UU ITE);
   2) Gangguan terhadap Sistem Elektronik (*system interference* – Pasal 33 UU ITE);
c. Tindak pidana memfasilitasi perbuatan yang dilarang (Pasal 34 UU ITE);
d. Tindak pidana pemalsuan informasi atau dokumen elektronik (Pasal 35 UU ITE);
e. Tindak pidana tambahan (*accessoir* Pasal 36 UU ITE); dan
f. Perberatan-perberatan terhadap ancaman pidana (Pasal 52 UU ITE).

Ketentuan Pidana *cybercrime illegal content* diatur dalam Pasal 45 ayat 1-5, Pasal 45A, dan Pasal 45B Undang-Undang No 19 Tahun 2016 tentang Perubahan Atas Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Adapun dalam Pasal 15 tentang penyelenggaraan Sistem Elektronik; 1) Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya. 2) Penyelenggara Sistem Elektronik bertanggung jawab terhadap Penyelenggaraan Sistem Elektroniknya. 3) Ketentuan sebagaimana dimaksud pada ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik. Dalam penjelasan Pasal 15 ayat (1) bahwa; "Andal" artinya Sistem Elektronik memiliki kemampuan yang sesuai dengan kebutuhan penggunaannya. "Aman" artinya Sistem Elektronik terlindungi secara fisik dan nonfisik.

"Beroperasi sebagaimana mestinya" artinya Sistem Elektronik memiliki kemampuan sesuai dengan spesifikasinya. Ayat (2) "Bertanggung jawab" artinya ada subjek hukum yang bertanggung jawab secara hukum terhadap Penyelenggaraan Sistem Elektronik tersebut. Kemudian dalam Pasal 26 tentang perlindungan hak pribadi diantaranya; a) Kecuali ditentukan lain oleh Peraturan Perundang-undangan, penggunaan, setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan. 2) Setiap orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini. Penjelasan Pasal 26 adalah; Dalam pemanfaatan Teknologi Informasi, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi *(privacy rights).* Hak pribadi mengandung pengertian sebagai berikut: a) Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan. b) Hak pribadi merupakan hak untuk dapat berkomunikasi dengan Orang lain tanpa tindakan memata-matai. c) Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang. Ayat (2) Cukup jelas. Dari beberapa penjelasan Pasal di atas menurut analisis penulis hanya menunjuk kepada perlindungan terhadap proses penyelenggaraan dan pemanfaatan Teknologi Informasi dan Transaksi Elektronik secara *preventif* (pencegahan) terjadinya korban tidak untuk melindungi korban. Mengenai perlindungan korban lebih jelasnya diatur dalam Undang-Undang No. 13 Tahun 2006 Tentang Perlindungan Saksi Dan Korban, Pasal 3 Perlindungan Saksi dan Korban berasaskan pada: a) Penghargaan atas harkat dan martabat manusia; b) Rasa aman; c) Keadilan; d) Tidak diskriminatif; dan e) Kepastian hukum.

3. Upaya yang Dilakukan Polrestabes Bandung Dalam Menanggulangi Adanya Korban Tindak Pidana *Cybercrime Illegal Content*

Dalam menanggulangi tindak pidana *cybercrime* yang mulai marak di Kota Bandung, pihak kepolisian melakukan upaya penanggulangan baik melalui upaya preventif dan represif. Upaya preventif adalah salah satu upaya penanggulangan terjadinya tindak pidana dengan mencegah perbuatan jahat seseorang untuk melakukan tindak pidana yang dilakukan sebelum terjadinya tindak pidana. Upaya preventif dilakukan melalui sarana di luar hukum pidana (non-penal). Penanggulangan melalui upaya preventif bertujuan untuk mengedukasi masyarakat agar tidak melakukan perbuatan yang dilarang guna menciptakan suasana yang kondusif untuk menekan terjadinya tindak pidana, termasuk dalam tindak pidana *cybercrime illegal content*. Berdasarkan hasil

wawancara, upaya-upaya yang dilakukan pihak Satreskrim Polrestabes Bandung melalui Iptu Ali Jupri, SH, MH. dan Aipda Teddy Yuliady antara lain : a) Melakukan pemblokiran terhadap situs-situs yang dianggap memiliki konten yang melanggar ketertiban dan kesusilaan, terdapat unsur teror yang meresahkan masyarakat, mengandung unsur tindak pidana atau dianggap merugikan masyarakat dengan kata lain mengandung konten bermuatan negatif yang bertentangan dengan perundang-undangan di Indonesia dengan berkoordinasi dengan pemerintah dan dalam hal ini juga diharapkan masyarakat dapat berpartisipasi dalam melakukan pemblokiran situs tertentu. b) Melalui kerjasama dan koordinasi dengan pemerintah untuk dan pihak terkait lainnya dalam rangka penegakan undang-undang yang dilakukan dengan sistematik dan terarah. c) Melalui sosialisasi ataupun penghimbauan kepada masyarakat melalui media cetak ataupun elektronik dalam bentuk bimbingan, pengarahan dan ajakan dari orang yang tidak dikenal, tidak mudah terpancing dengan barang murah yang dijual di internet dan juga agar lebih berhati-hati untuk menuliskan kritik ataupun bertutur kata di media sosial.

Upaya-upaya tersebut diharapkan dapat berjalan dengan efektif dan dapat memberikan pemahaman kepada masyarakat untuk berhati-hati. Upaya preventif diatas juga memberikan pemahaman kepada masyarakat bahwa siapa saja dapat menjadi korban tindak pidana *cybercrime* dan melalui sosialisasi pihak kepolisian menjelaskan mengenai sanksi tegas yang dapat diberikan kepada siapa saja yang melakukan tindak pidana *cybercrime*. Berdasarkan Pasal 5 ayat (3) Permenkominfo No. 19 Tahun 2014 tentang Penanganan Situs Internet Bermuatan Negatif, Lembaga Penegak Hukum dapat meminta pemblokiran situs bermuatan negatif kepada Direktur Jenderal yang membidangi aplikasi informatika. Jadi menurut penulis, langkah yang digunakan oleh pihak kepolisian sudah tepat tetapi perlu diperhatikan apakah pemblokiran sudah tepat sasaran atau belum. Penanggulangan tindak pidana *cybercrime* lainnya yaitu melalui upaya represif. Upaya represif atau sering disebut dengan penal yang dilakukan dengan menjatuhkan pidana guna menimbulkan efek jera kepada pelaku kejahatan sehingga tidak mengulangi perbuatannya. Upaya represif diterapkan setelah terjadinya tindak pidana.

Berdasarkan hasil wawancara dengan Iptu Ali Jupri, SH, MH. upaya penanggulangan secara represif terus dioptimalkan dengan menindaklanjuti setiap laporan tindak pidana yang dilaporkan ke pihak kepolisian. Setelah laporan diterima kemudian melakukan penyelidikan, setelah itu diserahkaan kepada penyidik untuk mulai mengumpulkan buktibukti hingga berkas dapat

dilimpahkan ke kejaksaan. Selanjutnya Iptu Ali Jupri, SH, MH. mengatakan bahwa diharapkan dengan memberikan sanksi yang tegas sesuai dengan peraturan perundang-undangan disertai dengan rasa keadilan dalam masyarakat dan kepastian hukum sehingga dapat memberikan efek jera kepada pelaku *cybercrime*. Polrestabes dan polsek di wilayah Kota Bandung juga dikerahkan ke garda terdepan dalam upaya menanggulangi kejahatan. Partisipasi masyarakat juga sangat dibutuhkan, tertuma dalam mengumpulkan bukti-bukti. Masyarakat diminta untuk sesegera mungkin melaporkan dan menyimpan seluruh rekaman atau data yang dapat mendukung kasus tersebut. Iptu Ali Jupri juga menjelaskan bahwa *cybercrime* merupakan kejahatan yang teroganisir karena jika dilihat dari latar belakang pendidikan tidak sebanding dengan keahliannya, sebelumnya para pelaku merupakan orang suruhan dari atasan mereka yang kemudian pelaku mempelajari apa yang telah didapatkan dari pengalaman bekerja dengan atasan mereka. Kendala dalam mengungkap kasus *cybercrime* ini telah dijelaskan sebelumnya oleh penulis yaitu mengenai keterbatasan alat yang dimiliki oleh pihak kepolisian, penghilangan barang bukti oleh pelaku, dan mengingat bahwa kasus *cybercrime* memiliki cakupan wilayah yang sangat luas tidak hanya antar provinsi di Indonesia tetapi juga lintas negara. Beberapa kendala tersebut di atas dapat mengurangi keefektifan gerak dan kegiatan pihak kepolisisan untuk menanggulangi kejahatan *cybercrime*, oleh karena itu pemenuhan atas kendala di atas dapat segera teratasi seperti koordinasi yang cepat dan terarah, pemenuhan alat-alat yang mendukung untuk melacak pelaku dan alat yang dapat mengembalikan kembali data yang hilang.

Untuk itu peran aktif masing-masing pihak sangat diperlukan dalam menanggulangi tindak pidana *cybercrime* dan pihak yang diberi tanggungjawab dapat melaksanakan tanggungjawabnya secara optimal dan diatasi dengan baik. *Cybercrime* merupakan kejahatan yang terjadi di wilayah maya atau virtual. Namun perlu diingat bahwa masyarakat yang berada di wilayah maya atau virtual tersebut adalah masyarakat nyata yang perlu mendapatkan perlindungan dan perhatian khusus oleh aparat penegak hukum. Penanggulangan merupakan langkah yang dapat digunakan untuk mencegah terjadinya pengulangan tindak pidana atau mengurangi angka kejahatan. Aparat penegak hukum juga berkewajiban untuk melindungi kepentingan korban *cybercrime* dan mengingatkan korban akan perannya yang dapat memberikan kesempatan kepada pelaku untuk melakukan kejahatan. Kerugian yang dialami korban *cybercrime* khususnya *illegal content* tidak hanya rugi secara materiil tetapi juga langsung kepada kondisi kejiwaan seseorang.

Setiap perbuatan pidana memiliki sanksi tegas yang telah diatur sebelumnya. Diharapkan dengan tegasnya sanksi yang diberikan kepada pelaku kejahatan dapat mencegah seseorang untuk melakukan perbuatan jahat atau dapat memberikan efek jera kepada para pelaku. Pelaku pada kasus *hacking* misalnya, setelah mendapat sanksi dapat juga diberi pengarahan berdasarkan kemampuannya untuk membantu pihak kepolisian mengungkap berbagai kasus yang berkaitan dengan *cybercrime* sehingga dapat memperbaiki kualitas hidupnya dan tidak mengulangi perbuatannya. Sehingga peran masyarakat, aparat penegak hukum dan pemerintah dapat berjalan sesuai tanggung jawabnya dan dijalankan berdasarkan rasa keadilan dan sebaik-baiknya. Dengan demikian, dapat disimpulkan bahwa upaya yang dilakukan polrestabes bandung dalam menanggulangi adanya korban tindak pidana *cybercrime illegal content* dilakukan dengan dua cara, yaitu melalui upaya preventif (pencegahan) dengan cara sosialisasi dan pemblokiran situs yang dianggap memiiliki muatan yang dilarang oleh undang-undang serta dengan upaya represif (penal) yang dilakukan dengan menjatuhkan pidana guna menimbulkan efek jera kepada pelaku kejahatan sehingga tidak mengulangi perbuatannya..

E. KESIMPULAN

Berdasarkan hasil uraian bab hasil penelitian dan pembahasan, maka penulis dapat menarik kesimpulan sebagai berikut:

1. Kedudukan korban dalam tindak pidana *cybercrime illegal content* di wilayah hukum Polrestabes Bandung adalah sebagai pihak yang secara hukum telah dilanggar hak-haknya menyangkut data pribadi/ kehormatan dirinya (*privacy)* karena suatu penghinaan, pencemaran nama baik, ataupun penyebaran konten asusila melalui media sosial/elektronik yang kebanyakan korbannya menimpa perempuan dan kedudukan hukumnya dalam proses persidangan, korban dijadikan sebagai alat bukti yang memberikan keterangan sebagai saksi.
2. Perlindungan hukum terhadap korban tindak pidana *cybercrime illegal content* menurut Undang-Undang No 19 Tahun 2016 tentang Perubahan Atas Undang-Undang No 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik tidaklah memuat secara *eksplisit* mengenai korban maupun perlindungan terhadap korban akan tetapi hanya memberikan perlindungan terhadap penyelenggara Teknologi Informasi dan Transaksi Elektronik seperti yang termuat dalam Pasal 4 tentang Asas dan tujuan

dalam poin (e) "memberikan rasa aman, keadilan, dan kepastian hukum bagi pengguna dan penyelenggara Teknologi Informasi"

3. Upaya penanggulangan yang dilakukan oleh pihak kepolisian di kota Bandung dilakukan dengan dua cara, yaitu melalui upaya preventif (pencegahan) dengan cara sosialisasi dan pemblokiran situs yang dianggap memiliki muatan yang dilarang oleh Undang-undang serta dengan upaya represif (penal). Namun dari kedua upaya yang dilakukan pihak kepolisian, belum dapat mengurangi kasus *cybercrime illegal content* yang setiap tahun mengalami peningkatan. Upaya represif dengan menindaklanjuti setiap kasus yang dilaporkan belum dapat dioptimalkan karena terdapat beberapa kendala yang dihadapi. Kendala tersebut antara lain, kurangnya alat penunjang yang dimiliki oleh kepolisian dan pelaku yang kerap menghilangkan barang bukti.

DAFTAR PUSTAKA

Buku:

A.S. Alam & Amir Ilyas. *Pengantar Kriminologi*. Pustaka Refleksi Books: Makasar, 2010.

Arif Gosita. *Masalah Korban Kejahatan (Kumpulan Karangan).* Akademika Pressindo: Jakarta, 1993.

Bambang Waluyo, *Viktimologi Perlindungan Korban dan Saksi,* Jakarta, 2011

Barda Nawawi Arief. *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime Di Indonesia*. PT Raja Grafindo Persada: Jakarta, 2006.

Budi Suhariyanto. *Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya.* Rajawali Pers: Jakarta, 2013.

Dikdik M. Arief & Elisatris Gultom. *Cyber Law,* cet. II. Refika Aditama: Bandung, 2009.

Edmon Makarim. *Pengantar Hukum Telematika,* cet. I. PT Raja Grafindo Persada: Jakarta, 2005.

Mansur, Dikdik M. Arief & Elisatris Gultom. *Urgensi Perlindungan Korban Kejahatan*. PT. Raja Grafindo Persada: Jakarta, 2007.

Martin Steinmnan & Gerald Willen. *Metode Penulisan Skripsi dan Tesis.* Angkasa: Bandung, 1974.

Maskun. *Cybercrime Cybercrime Suatu Pengantar".* Kencana: Jakarta, 2013.

R Soesilo, *Kitab Undang-Undang Hukum Pidana (KUHP) Serta Komentar-Komentarnya,* Politeia: Bogor. 1995.

Rena Yulia. *Viktimologi Perlindungan Hukum Terhadap Korban Kejahatan,* Graha Ilmu, Yogyakarta. 2010.

Siswanto Sunarso. *Hukum Informasi dan Transaksi Elektronik.* Rineka Putra: Jakarta. 2009.

Sitompul, Josua. *Cyberspace, Cybercrimes, Cyberlaws: Tinjauan Hukum Pidana*. PT Tatanusa: Jakarta. 2012.

Sudarsono. *Kamus Hukum*. PT Rineka Cipta: Jakarta. 2007.

Peraturan Perundang-undangan:

Undang-Undang Dasar 1945

Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang No. 19 Tahun 2016 tentang Perubahan Atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang No. 13 Tahun 2006 Tentang Perlindungan Saksi Dan Korban

Undang-Undang No. 8 Tahun 1981 tentang Hukum Acara Pidana.

Undang-Undang No. 1 Tahun 1946 tentang Hukum Pidana.

Website:

http://www.merdeka.com/peristiwa/hasil-riset-hukum-tahun-2013-Indonesia-target-utama-kejahatan-cyber.httml, diakses pada 15 Maret 2017.

http://library.unej.ac.id/client/en_US/default/search/asset/632?dt=list M. Arief Amrullah, Makalah: "Perkembangan Studi Tentang Korban dan Kedudukannya Dalam Hukum Pidana Positif", hlm. 4. Diakses pada 20 Maret 2017

http://pustaka.uns.ac.id/download/Dr.%20Pujiyono.%20SH.%20MH.docx Pujiyono, Makalah: "Eksistensi Hukum Pidana Dalam Menanggulangi Cyber Crime di Indonesia, hlm. 13-15 diakses pada 21 Maret 2017.